Cybersecurity in the Banking Industry: African Case Studies

Case studies by:
Prof. Francis Wambalaba, United States International University (USIU)
Dr. Paula Musuva, United States International University (USIU)
Judy Ouma, Technical University of Kenya
William Makatiani, Serianu Limited
Brencil Kaimba, Serianu Limited
Dr. Koussis Nicos, Fredrick University

SWIFT INSTITUTE

Security and risk experts within African organisations have identified methodologies and frameworks for minimising and quantifying their risks within their limited budgets.

Introduction

The financial sector has always been a primary target for cyber-attacks and it is imperative that cyber risk minimisation practices within financial institutions remain resilient to cyber threats.

Organisations in Africa are faced with numerous attacks against their infrastructure, however, with limited budgets to support risk minimisation efforts most risk experts are usually unable to deploy the right skills and tools.

A recent Africa Cybersecurity Report states that up to 80% of organisations in Africa spend less than USD 10,000 on cybersecurity annually.

While innovative technologies are key in a competitive market, there also needs to be a corresponding investment in the development and enforcement of policy guidelines to safeguard operational environments.

There have been commendable advancements in the enactment of cybercrime and data protection legislation by East African countries following the establishment of the 2014 African Union Convention on Cyber Security and Personal Data Protection. However, it is important for policy makers and governance professionals within the banking industry to understand the impact any lag between technology and policy has on cyber security.

Through a partnership between The SWIFT Institute and The Global Business School Network (GBSN)* two research case studies have been developed looking at cybersecurity and banking across the African and specifically East African context.

Case studies

1.

Cybersecurity Risk Minimisation Best Practices — African Experiences:

Identifies key cyber security risks, cyber security risk quantification and minimisation practices in the banking industry. Taking a comparative view, it highlights the African experience, and provides mitigating measures and strategies for cyber security risk minimisation on emerging areas of concern for African financial institutions.

2.

Cybersecurity Risks and National Policy Implications — East African Experiences:

Assesses the cybersecurity risks stemming from lags between policy development and technological advances in the banking industry with particular focus on the East African Region.

Key takeaways across the case studies

Cybersecurity threats

- Organisations in Africa are faced with numerous attacks against their infrastructure, however, with limited budgets to support risk minimization efforts most risk experts are usually unable to deploy the right skills and tools.
- With regards to cybersecurity risk, banks are facing huge risks relating to financial fraud, data theft and malware attacks. The greatest source of these risks are malicious insiders and local organised crime syndicates.
- Insider threat causes the largest security losses, and is the hardest to detect, remediate and prosecute. Insiders constitute employees, vendors or contractors.
- Organised crime syndicates are not only on the increase in terms of geographical reach but also in the number of collusions with malicious insiders with the objective of launching sophisticated attacks.

How are institutions responding?

- By deploying various detective and preventive measures to deter and protect their assets from cyber-attacks.
- By implementing Information Security Policies to support risk management and security education training and awareness.
- By adopting various frameworks to streamline their cyber risk management processes to benchmark with industry standards. To date, ISO 27001 is the most adopted industry framework. The paper discusses ISO, NIST, PCI-DSS and the SWIFT Customer Security Programme.

What role is technology playing?

- Over the period 2010 to 2017, USD $722 million was invested into FinTech in East Africa, with Kenya receiving the largest investment.
- In the East African banking industry, the top five technology advancements are: mobile banking, online banking, open banking, bank assurance and cloud computing.
- Drivers for the adoption of these technology innovations are to:
  - provide faster access to 24/7 banking services
  - increase operational efficiencies
  - drive down costs

Technology to mitigate cyber risks

- The research surveys indicated that the technology controls that East African banks have found to be essential relate to network firewalls, anti-malware solutions, backups, domain access management, information security policies, system auditing and monitoring, security education training and awareness and log management.
- Those least implemented included data classification, digital forensics and Security Operation Centres (SOC).
- Essential processes to mitigate cyber risks relate to logical access and password policies, anti-malware solutions, regular patch management (combined with regular vulnerability scanning) penetration testing, risk assessments and cyber incident response through a coordinated response team and security operations centre.

What role has regulation played?

- There have been commendable advancements in the enactment of cybercrime and data protection legislation by East African countries following the establishment of the 2014 African Union Convention on Cyber Security and Personal Data Protection.
- Such legislation makes it possible to prosecute cybercriminals and act as a deterrent factor when enforced.
- Regards enhancing cyber risk management practices in the banking sector, the Central bank guidelines have played a key role, closely followed by the data protection laws passed within the same countries. These regulations and guidelines outline minimum security measures that organisations should implement to protect customer assets.
- Equally the regulatory push has elevated the importance of cyber-awareness to board-level, whereby there has been an increased need for Chief Information Security Officers (CISOs) to fully quantify and explain the organisations' cybersecurity posture and exposures.
- Cyber risk quantification is a fairly new concept in Africa. Various frameworks have been designed specifically to assist CISOs and security teams to quantify their risks and present this data in a clear and quantifiable manner.
- Despite potential benefits in mitigating cybersecurity risks and fighting fraud, East African banks have not yet operationalised artificial intelligence and in general have a negative perception of blockchain technologies.

Conclusion

The studies highlight that a number of challenges remain to be addressed, such as greater investment in human resource development across organisations, policy makers and law enforcers to guide the changing face of technology innovation and to avert potential cybersecurity risks.

The need for greater co-operation between FinTech innovators and regulatory bodies is clearly flagged, however on a positive note, regulators are adopting models such as FinTech observation techniques in controlled sandbox environments. There is a clear intention not to stifle innovation, and ensure policy guidelines are well informed to avert negative outcomes and cybersecurity risks.

Security and risk experts within African organisations have identified methodologies and frameworks for minimising and quantifying their risks within their limited budgets. Overall, cyber security risk minimisation has to be seen as a never-ending challenge that will require African organisations to continuously adapt and tackle.

These two case studies developed by GBSN will be used in business schools across Africa to teach the next generation of cyber security professionals. In the short-term, they offer good insights and guidance for financial institutions on how to continue the fight against cyber-crime.

*About the Global Business School Network: GBSN is a non-profit organization that partners with business schools, industry, foundations and aid agencies to improve access to quality, locally relevant management education for the developing world.

The SWIFT Institute, set up by SWIFT, funds independent research, supports knowledge-led debate and provides a forum where academics and financial practitioners can learn from each other.